On the Sato Conjecture for QM-curves of genus two(Analytic Number Theory)

AUTHOR(S):

TSUNOGAI, Hiroshi

CITATION:

TSUNOGAI, Hiroshi. On the Sato Conjecture for QM-curves of genus two(Analytic Number Theory). 数理解析研究所講究録 1996, 958: 129-140

ISSUE DATE:

1996-08

URL:

http://hdl.handle.net/2433/60455

数理解析研究所講究録
958巻 1996年 129-140

On the Sato Conjecture for QM-curves of genus two

TSUNOGAI Hiroshi (角谷宏 早稲田大理工)

This is a joint work with Ki-ichiro Hashimoto (Waseda University), and will appear as [HT].

0. Introduction

In this article we shall report a computational result about the distribution of the arguments of zeroes of L-functions of two-dimensional abelian varieties with quaternionic multiplication (QM). The result we obtained supports an analogue of the Sato Conjecture for such abelian surfaces.

An abelian surface A is called a *QM-abelian surface* if it has quaternionic multiplication, that is, there exists an order $\mathcal{O}$ of an indefinite quaternion algebra $\boldsymbol{B}$ over $\boldsymbol{Q}$ and an embedding $\iota : \mathcal{O} \hookrightarrow \mathrm{End}A$. A curve C of genus two is called a *QM-curve* if its jacobian variety is a QM-abelian surface.

In [HM] K. Hashimoto and N. Murabayashi obtained algebraic families of QM-curves explicitly when the discriminants of $\boldsymbol{B}$ are 6 and 10. In the case of discriminant 6, the following equations give a family of QM-curves:

(0.1)
$$\mathcal{S}_6(t,s) : Y^2 = X(X^4 + (A-B)X^3 + QX^2 + (A+B)X + 1),$$
$$A = \frac{s}{2t}, \quad B = \frac{1+3t^2}{1-3t^2},$$
$$Q = -\frac{(1-2t^2+9t^4)(1-28t^2+166t^4-252t^6+81t^8)}{4t^2(1-3t^2)^2(1-t^2)(1-9t^2)},$$

(0.2)
$$S_{\boldsymbol{B}_6} : g(t,s) = s^2 + 3 - 14t^2 + 27t^4 = 0.$$

(This is slightly modified from the form in *loc.cit.* We have obtained another family which has different arithmetic properties. See Remark 3.3) By specializing (t,s) to points $(t_0,s_0) \in S_{\boldsymbol{B}_6}(\bar{\boldsymbol{Q}})$, we can obtain a lot of examples of QM-curves defined over number fields.

For many examples of QM-curves, we calculated the congruence ζ-functions of their reductions modulo $\mathfrak{p}$ and studied the distribution of the argument of the roots α, β of the characteristic polynomial of the Frobenius endomorphisms.

For a curve C of genus two defined over a number field k, the congruence ζ-function of C mod $\mathfrak{p}$ for a good prime $\mathfrak{p}$ of k can be written in the form

$$Z(u) = \frac{(1-\alpha u)(1-\bar{\alpha}u)(1-\beta u)(1-\bar{\beta}u)}{(1-u)(1-qu)}, \tag{0.3}$$

where $^-$ denotes the complex conjugate, the absolute values of α, β are $\sqrt{q}$, and $q = N\mathfrak{p}$, the absolute norm of $\mathfrak{p}$. In our case of QM-curves, if all endomorphisms of Jac$C$ are defined over k, we have $\alpha = \beta$. Put $\alpha = \sqrt{q}e^{i\theta_\mathfrak{p}}$ with $\theta_\mathfrak{p} \in [0, \pi]$. On the distribution of $\{\theta_\mathfrak{p}\}$ there is a conjecture as an analogue of the Sato Conjecture for elliptic curves. Let us explain them.

The original *Sato Conjecture* is as follows. Let E be an elliptic curve defined over a number field k. For a good prime $\mathfrak{p}$ of k, the congruence ζ-function of E mod $\mathfrak{p}$ is in the form

$$Z(u) = \frac{(1-\sqrt{q}e^{i\theta_\mathfrak{p}}u)(1-\sqrt{q}e^{-i\theta_\mathfrak{p}}u)}{(1-u)(1-qu)}, \tag{0.4}$$

where $\theta_\mathfrak{p} \in [0, \pi]$. M. Sato conjectured that if E has no complex multiplication the arguments $\{\pm\theta_\mathfrak{p}\}$ would be distributed in proportion to $\sin^2\theta$. Also J. Tate arrived to this conjecture and noticed in [T].

H. Yoshida[Yo1] generalized the above conjecture for higher-dimensional abelian varieties A. He conjectured that the distribution of the arguments is characterized by the image of the Galois group under the l-adic representation (more precisely, the Mumford-Tate group) of A. By Faltings' theorem [F], for a QM-abelian surface A defined over a number field k, the image of the l-adic representation associated to A is a subgroup of GSp(2) isomorphic to GL(2) (up to finite index). This suggests the following conjecture for the case of QM-abelian surfaces:

Conjecture. *Let A be a QM-abelian surface defined over a number field k. Assume that also all endomorphisms of A are defined over k. For a good prime $\mathfrak{p}$ of k, let $\pm\theta_\mathfrak{p}$ be the arguments of the eigenvalues of the Frobenius endomorphisms of A mod $\mathfrak{p}$. Then $\{\pm\theta_\mathfrak{p}\}$ would be distributed in proportion to* $\sin^2\theta$.

Preceedingly Y. Yamamoto reported in [Ya] a result of computation which fits with the generarized conjecture for abelian surfaces A with End$A \simeq \boldsymbol{Z}$.

H. Yoshida[Yo2] proved an analogue of these conjectures for the cases of elliptic curves and QM-abelian surfaces over a function field over a finite field.

If C is a QM-curve, then $A = \mathrm{Jac}C$ is a QM-abelian surface, and the eigenvalues of Frobenius endomorphisms of A mod $\mathfrak{p}$ coincide with the zeroes of the congruence ζ-function of C mod $\mathfrak{p}$. Hence we can examine the conjecture by calculating the congruence ζ-function of C mod $\mathfrak{p}$. We calculated them for

more than twenty curves C and for primes $\mathfrak{p}$ with $N\mathfrak{p} < 2^{20}$, and obtained the results which support the conjecture.

We carried out these calculation on PC with UBASIC and on UNIX Work Station with GNU C. We thanks voluntary helpers of the computer room of our department and stuffs of Centre for Informatics, Waseda University. Especially we would like to express our sincere gratitude to Kazumaro Aoki for useful suggestions for improving algorithm.

1. Congruence ζ-functions

First recall basic facts about congruence ζ-functions. For a curve C over $\boldsymbol{F}_q$, let N_m denote the number of $\boldsymbol{F}_{q^m}$-rational points on C. The *congruence ζ-function* of C is defined to be

$$Z(C/\boldsymbol{F}_q; u) = \exp\left(\sum_{m=1}^{\infty} \frac{N_m}{m} u^m\right). \tag{1.1}$$

Let C be a complete, non-singular curve of genus two. Then, by Weil conjecture, we have

$$Z(C/\boldsymbol{F}_q; u) = \frac{P(u)}{(1-u)(1-qu)}, \tag{1.2}$$

where $P(u) \in \boldsymbol{Z}[u]$ is of degree 4, and $P(u) = (1-\alpha u)(1-\bar{\alpha}u)(1-\beta u)(1-\bar{\beta}u)$ with $|\alpha| = |\beta| = \sqrt{q}$. By putting $\alpha + \bar{\alpha} = a$ and $\beta + \bar{\beta} = b$, we can write

$$P(u) = (1 - au + qu^2)(1 - bu + qu^2) \tag{1.3}$$

with $a, b \in \boldsymbol{R}$ and $|a|, |b| \leq 2\sqrt{q}$. From (1.1) and (1.3), a and b are evaluated as

$$\begin{cases} a + b = 1 + q - N_1, \\ ab = -q - (1+q)N_1 + \dfrac{1}{2}(N_2 + N_1^2). \end{cases} \tag{1.4}$$

Let $J = \mathrm{Jac}C$ be the Jacobian variety of C over $\boldsymbol{F}_q$, l a prime different from the characteristic of $\boldsymbol{F}_q$, and ρ_l the l-adic representation:

$$\rho_l : \mathrm{Gal}(\bar{\boldsymbol{F}}_q/\boldsymbol{F}_q) \longrightarrow \mathrm{GSp}(4, \boldsymbol{Z}_l). \tag{1.5}$$

Then, for Frobenius element σ, the characteristic polynomial of $\rho_l(\sigma)$ does not depend on l and coincides with $P(u)$.

Let C be a QM-curve over a number field k, $J = \mathrm{Jac}C$ its Jacobian, $\mathcal{O}$ an order of an indefinite quaternion algebra $\boldsymbol{B}$ over $\boldsymbol{Q}$ identified with $\mathrm{End}J$. Take a good prime $\mathfrak{p}$ of k and let p be its residue characteristic and $N\mathfrak{p} = q$. For a prime number l different from p, we denote the associated completion of $\mathcal{O}$ (resp. $\boldsymbol{B}$) by $\mathcal{O}_l$ (resp. $\boldsymbol{B}_l$). Then we have $\mathrm{End}T_lJ \otimes_{\boldsymbol{Z}_l} \boldsymbol{Q}_l \simeq \mathrm{M}_4(\boldsymbol{Q}_l)$. Let

k' be an extension of k over which all endomorphisms of J are defined. First, consider the l-adic representation ρ_l attached to J of $\mathrm{Gal}(\bar{\boldsymbol{Q}}/k')$:

$$\rho_l : \mathrm{Gal}(\bar{\boldsymbol{Q}}/k') \longrightarrow \mathrm{GSp}(4, \boldsymbol{Z}_l) \subset \mathrm{M}_4(\boldsymbol{Q}_l). \tag{1.6}$$

Denote by $\mathrm{End}_{\mathrm{Gal}(\bar{k}/k')}T_lJ$ the centralizer of $\mathrm{Im}\rho_l$ in $\mathrm{End}T_lJ$. Then, by Faltings [F], $\mathrm{End}_{\mathrm{Gal}(\bar{k}/k)}T_lJ \otimes_{\boldsymbol{Z}_l} \boldsymbol{Q}_l \simeq \mathrm{End}_{k'}J \otimes \boldsymbol{Q}_l = \boldsymbol{B}_l$. Hence $\mathrm{Im}\rho_l$ is contained in the centralizer of $\boldsymbol{B}_l$ in $\mathrm{M}_4(\boldsymbol{Q}_l)$, which is isomorphic to the opposite algebra $\boldsymbol{B}_l^0$ of $\boldsymbol{B}_l$. For a prime $\mathfrak{P}$ of k' above $\mathfrak{p}$, let $\sigma_{\mathfrak{P}}$ be the Frobenius element. Since $\rho_l(\sigma_{\mathfrak{P}})$ belongs to $\boldsymbol{B}_l^0$, it satisfies a quadratic relation in the form

$$1 - c_{\mathfrak{P}}X + (N\mathfrak{P})X^2 = 0. \tag{1.7}$$

Now consider ρ_l on $\mathrm{Gal}(\bar{\boldsymbol{Q}}/k)$. Let $f = f(\mathfrak{P}/\mathfrak{p})$ be the inertia degree of $\mathfrak{P}$ in k'/k. Then $\rho_l(\sigma_{\mathfrak{p}})$ satisfies

$$1 - c_{\mathfrak{P}}X^f + (qX^2)^f = 0 \tag{1.8}$$

since $\sigma_{\mathfrak{P}} = \sigma_{\mathfrak{p}}^f$. On the other hand, since $\rho_l(\sigma_{\mathfrak{p}})$ belongs to $\mathrm{M}_4(\boldsymbol{Q}_l)$, it satisfies a quartic relation. From this we find a relation which must be satisfied by N_1 and N_2, for each possible value of f. Hence we can determine the degree f from the values N_1 and N_2. For example, if $f = 1$ then the characteristic polynomial of $\rho_l(\sigma_{\mathfrak{p}})$ is $(1 - c_{\mathfrak{P}}X + qX^2)^2 = (1 - a_{\mathfrak{p}}X + qX^2)^2$ with $a_{\mathfrak{p}} = c_{\mathfrak{P}}$. By (1.4), we have

$$(1 + q - N_1)^2 = 2(1 + 4q + q^2 - N_2), \quad a_{\mathfrak{p}} = \frac{1}{2}(1 + q - N_1). \tag{1.9}$$

If $f = 2$ then the characteristic polynomial of $\rho_l(\sigma_{\mathfrak{p}})$ is $1 - c_{\mathfrak{P}}X^2 + q^2X^4 = (1 - a_{\mathfrak{p}}X + qX^2)(1 + a_{\mathfrak{p}}X + qX^2)$ with $a_{\mathfrak{p}}^2 = c_{\mathfrak{P}} + 2q$. By (1.4), we have

$$N_1 = 1 + q, \quad a_{\mathfrak{p}}^2 = \frac{1}{2}(1 + 4q + q^2 - N_2). \tag{1.10}$$

Also for $f > 2$ we have the relation between N_1 and N_2.

Now one of the remarkable properties for our family $\mathcal{S}_6$ given in (0.1) is that (numerically) we always have $f = 1$. This shows that all endomorphisms of $\mathrm{Jac}C$ are defined over the field of definition of C in quite a large probability, because, if almost all primes of a number fields k decomposed completely in an extention k'/k then $k' = k$. Based on this assumption, for following many primes, we calculated only N_1 to obtain results in reasonable time.

2. Density functions

Let $\Theta = \{\theta_j\}_{j=1}^{\infty}$ be a sequence in $T = \boldsymbol{R}/2\pi\boldsymbol{Z}$, the unit circle. A real valued distribution $\Phi = \Phi(\theta)$ on T is called the *density function* of Θ if it has the following property:

For any open interval U of T and any natural number m, let

$$n(U,m) = \#\{j \in \boldsymbol{N} | \theta_j \in U, j < m\}. \tag{2.1}$$

Then it holds that

$$\lim_{m\to\infty} \frac{n(U,m)}{m} = \int_U \Phi(\theta)d\theta, \tag{2.2}$$

where $d\theta$ denotes the measure on T induced from the Lebesgue measure on $\boldsymbol{R}$.

Next lemma is basic (see, e.g. [Yo2]).

Lemma 2.1. *For a sequence $\Theta = \{\theta_j\}_{j=1}^{\infty}$ on T, assume that*

$$c_k = \lim_{m\to\infty} \frac{1}{2\pi m} \sum_{j=1}^{m} e^{-ik\theta_j}$$

exists for all $k \in \boldsymbol{Z}$. Then

$$\Phi(\theta) = \sum_{k=-\infty}^{\infty} c_k e^{ik\theta}$$

converges in the sense of distribution and is the density function of Θ.

Let E be an elliptic curve defined over a number field k. For a good prime $\mathfrak{p}$ of k, let $\pm\theta_{\mathfrak{p}}$ be the arguments of zeroes of the congruence ζ-function for E mod $\mathfrak{p}$ (see (0.4)). Since we should consider the distribution of a sequence of pairs $\Theta = \{\pm\theta_{\mathfrak{p}}\}_{\mathfrak{p}}$, we define the density function of Θ as a distribution satisfying

$$\lim_{x\to\infty} \frac{\#\{\pm\theta_{\mathfrak{p}} \in U | N\mathfrak{p} < x\}}{\#\{\pm\theta_{\mathfrak{p}} | N\mathfrak{p} < x\}} = \int_U \Phi(\theta)d\theta. \tag{2.3}$$

The original Sato Conjecture asserts that, if E has no complex multiplication, then it would hold that $\Phi(\theta) = \pi^{-1}\sin^2\theta$.

Let C be a QM-curve defined over a number field k. We assume that also all endomorphisms of Jac$C$ are defined over k. Then, for a good prime $\mathfrak{p}$ of k, the congruence ζ-function of C mod $\mathfrak{p}$ is in the form

$$Z(u) = \frac{(1-\sqrt{q}e^{i\theta_{\mathfrak{p}}}u)^2(1-\sqrt{q}e^{-i\theta_{\mathfrak{p}}}u)^2}{(1-u)(1-qu)}, \tag{2.4}$$

where $q = N\mathfrak{p}$ is the absolute norm of $\mathfrak{p}$. Similarly to the case of an elliptic curve, we consider the density function of the pairs $\Theta = \{\pm\theta_{\mathfrak{p}}\}_{\mathfrak{p}}$. A generalization of the Sato Conjecture by H. Yoshida asserts that the density function Φ of Θ would be

$$\Phi(\theta) = \pi^{-1}\sin^2\theta. \tag{2.5}$$

We checked this conjecture for many QM-curves of discriminant 6 by calculating Fourier coefficients of $\Phi(\theta)$ approximately. Similarly to Lemma 2.1, we have the following lemma.

Lemma 2.2. *For $\Theta = \{\pm\theta_{\mathfrak{p}}\}_{\mathfrak{p}}$, assume that the limit*

$$c_k := \lim_{x\to\infty} \frac{1}{\#\{\mathfrak{p}|\textit{good prime}, N\mathfrak{p} < x\}} \sum_{N\mathfrak{p}<x} \cos k\theta_{\mathfrak{p}}$$

exists for all positive integer k. Then

$$\Phi(\theta) = \frac{1}{2\pi} + \frac{1}{\pi}\sum_{k=1}^{\infty} c_k \cos k\theta$$

converges in the sense of distribution and is the density function of Θ.

If the conjecture is true, then the Fourier coefficients c_k of Φ must be

$$c_2 = -\frac{1}{2}, \quad c_k = 0 \ (k \neq 2). \tag{2.6}$$

We calculated approximate values of c_k's as

$$c_k \fallingdotseq \frac{1}{\#\{\mathfrak{p}|\text{good prime}, N\mathfrak{p} < x\}} \sum_{N\mathfrak{p}<x} \cos k\theta_{\mathfrak{p}} \tag{2.7}$$

for sufficiently large x.

Remark 2.3. In the definition of Fourier coefficients c_k, we can restrict primes to those of degree one. But we calculated the arguments $\pm\theta_{\mathfrak{p}}$ also for primes $\mathfrak{p}$ of degree more than one (in fact, of degree two because we examined QM-curves defined over (imaginary) quadratic fields) to check the absence of qualitative difference.

3. Results

(3.1)
$$\mathcal{S}_6(t,s) : Y^2 = X(X^4 + (A-B)X^3 + QX^2 + (A+B)X + 1),$$
$$A = \frac{s}{2t}, \quad B = \frac{1+3t^2}{1-3t^2},$$
$$Q = -\frac{(1-2t^2+9t^4)(1-28t^2+166t^4-252t^6+81t^8)}{4t^2(1-3t^2)^2(1-t^2)(1-9t^2)},$$

(3.2)
$$S_{B_6} : g(t,s) = s^2 + 3 - 14t^2 + 27t^4 = 0.$$

We denote by $C_{(t_0,s_0)}$ the curve obtained by specializing (t,s) to a point (t_0,s_0) on $g(t,s)=0$. We can find that $C_{(t,s)} = C_{(-t,-s)}$ and that $C_{(t,s)}$ and $C_{(t,-s)}$ are generically isomorphic over $\boldsymbol{Q}(\sqrt{-1})$ by

(3.3)
$$C_{(t,s)} \simeq C_{(t,-s)}$$
$$(X,Y) \leftrightsquigarrow (-X^{-1}, \sqrt{-1}X^{-3}Y).$$

We checked the following curves and primes:

(3.4)
$$t \in \boldsymbol{Z},\ 2 \le t \le 30\ (\#=29)$$
$$N\mathfrak{p} < 2^{20} \text{ (primes of degree one)}.$$

Since $t \in \boldsymbol{Q}$, $C_{(t,s)}$ is defined over an imaginary quadratic field $k = \boldsymbol{Q}(s) = \boldsymbol{Q}(\sqrt{-t^2-3})$. Moreover $C_{(t,s)}$ and $C_{(t,-s)}$ are conjugate over $\boldsymbol{Q}$. If a rational prime p decomposes as $p = \mathfrak{p}\mathfrak{p}'$ in k, then

(3.5)
$$C_{(t,s)} \bmod \mathfrak{p}' \simeq C_{(t,-s)} \bmod \mathfrak{p} \text{ (over } \boldsymbol{F}_p)$$
$$\simeq C_{(t,s)} \bmod \mathfrak{p} \text{ (over } \boldsymbol{F}_p(\sqrt{-1})),$$

where $\boldsymbol{F}_p(\sqrt{-1})$ means $\boldsymbol{F}_p$ if $p \equiv 1 \bmod 4$ or $\boldsymbol{F}_{p^2}$ if $p \equiv 3 \bmod 4$. Hence we have $\theta_{\mathfrak{p}'} = \theta_{\mathfrak{p}}$ if $p \equiv 1 \bmod 4$ or $\theta_{\mathfrak{p}'} = \pi - \theta_{\mathfrak{p}}$ if $p \equiv 3 \bmod 4$. This allows us that we may consider only one prime above p for a splitting prime p.

For each curve $C = C_{(t,s)}$, we first computed the numbers of $\boldsymbol{F}_p$- and $\boldsymbol{F}_{p^2}$-rational points of C mod $\mathfrak{p}$ for first thirty splitting primes $\mathfrak{p}$ of k to check the assumption that all endomorphisms of Jac$C$ are defined over k, and obtained the data which shows the assumption is true. Under this assumption, the congruence ζ-function of C mod $\mathfrak{p}$ is determined only by the number N_1 of $\boldsymbol{F}_p$-rational points. We computed N_1 of C mod $\mathfrak{p}$ for splitting primes $\mathfrak{p}$ of k with $N\mathfrak{p} < 2^{20}$ (more than 40000 primes), and calculated the approximate values of

the Fourier coefficients c_k of the density function by (2.7). For all curves we checked, all the approximate values of c_k satisfy

$$(3.6) \qquad |c_2 + \frac{1}{2}| < 0.007, \quad |c_k| < 0.011 \quad (k > 0, k \neq 2).$$

In fact, out of 551 values of $|c_k|$ $(k > 0, k \neq 2)$, only 49 values are bigger than 0.005. For c_2, out of 29 values of $|c_2 + \frac{1}{2}|$, only 2 values are bigger than 0.005. We also computed for remain primes $\mathfrak{p} = (p)$ of k with $N\mathfrak{p} < 2^{20}$ $(p < 2^{10})$, which showed no qualititive difference from splitting primes.

We shall give precise data for $t = 2, 3$ in the following. In the examples, Table A gives the approximate values of Fourier coefficients of the density function and Table B gives the frequency distribution of the arguments and the comparison with $\sin^2\theta$.

Example 1.

$$C_{(2,\sqrt{-379})} : Y^2 = X(X^4 + (\frac{\sqrt{-379}}{4} + \frac{13}{11})X^3 - \frac{979961}{203280}X^2 + (\frac{\sqrt{-379}}{4} - \frac{13}{11})X + 1)$$

We calculated for 40823 splitting primes (Table 1.A, 1.B, Figure 1.C).

Example 2.

$$C_{(3,4\sqrt{-129})} : Y^2 = X(X^4 + (\frac{2\sqrt{-129}}{3} + \frac{14}{13})X^3 - \frac{1003831}{60840}X^2 + (\frac{2\sqrt{-129}}{3} - \frac{14}{13})X + 1)$$

We calculated for 40994 splitting primes (Table 2.A, 2.B).

The following example is the case that Jac$C$ is isogenous to a product $E \times E$ of an elliptic curve E with complex multiplication.

Example 3 ([HM] *Example 2.5*).

$$C_{(\frac{\sqrt{-3}}{3}, \frac{4\sqrt{-6}}{3})} : Y^2 = X(X^4 + 2\sqrt{2}X^3 + \frac{11}{3}X^2 + 2\sqrt{2} + 1)$$

Via the following morphism ϕ of degree two, Jac$C$ splits into $E \times E$:

$$(3.7) \qquad \phi : C_{(\frac{\sqrt{-3}}{3}, \frac{4\sqrt{-6}}{3})} \longrightarrow E : y^2 = (x+2)(x^2 + 2\sqrt{2}x + \frac{5}{3})$$

$$(X, Y) \longmapsto (x, y) = (X + \frac{1}{X}, \frac{Y(X+1)}{X^2}),$$

where E is an elliptic curve with complex multiplication by $\boldsymbol{Z}[\sqrt{-6}]$, whose invariant is $j(\sqrt{-6}) = 12^3(1399 + 988\sqrt{2})$.

We calculated for 41003 splitting primes (Table 3.A, 3.B).

Remark 3.1. In this case the Hasse-Weil L-function of C coincides with a square of that of E. For the primes inert in $\boldsymbol{Q}(\sqrt{2},\sqrt{6})/\boldsymbol{Q}(\sqrt{2})$ (density $\frac{1}{2}$), the arguments of zeroes of the characteristic polynomials of the Frobenius elements are all $\frac{\pi}{2}$, and for the primes splitting in $\boldsymbol{Q}(\sqrt{2},\sqrt{6})/\boldsymbol{Q}(\sqrt{2})$ they are distributed uniformly on T by the property of größencharacter. Hence the k-th Fourier coefficients of the density function $\Phi(\theta)$ must be $\frac{(-1)^{\frac{k}{2}}}{2}$ for even k and zero for odd k. The data above fits with this fact very well.

Remark 3.2. By similar argument to [HM] Example 1.6, we can *prove* that, in Examples 1 and 2, Jac$C$ are *simple* QM-abelian surfaces, i.e. they never split into a product of CM-elliptic curves. The qualitative difference between these examples and Example 3 is so clear that we can distinguish experimantally whether Jac$C$ is simple or not.

Remark 3.3. The family of QM-curves $\mathcal{S}_6(t,s)$ has an automorphism w of order two which preserves fibration and is defined over $\boldsymbol{Q}$, described as

$$w : (t,s,X,Y) \longmapsto (-\frac{1}{3t}, -\frac{s}{3t}, X^{-1}, X^{-3}Y). \tag{3.8}$$

Hence we obtain another family $\mathcal{S}_6^0(t,s) = \mathcal{S}_6(t,s)/\langle w\rangle$ of QM-curves over a curve $S_{B_6}^0 = S_{B_6}/\langle w\rangle$ by dividing it by $\langle w\rangle$. Its defining equation is

(3.9)

$$\begin{aligned}\mathcal{S}_6^0(t,s) : Y^2 &= (X^2-R)\{(2-Q+2A)X^4 - 4RX^3 \\ &\qquad + 2R(6+Q)X^2 + 4R^2X + R^2(2-Q-2A)\},\\ A &= \frac{s}{t}, \quad R = 1+3t^2,\\ Q &= \frac{(1+t^2)(1-4t^2+t^4)}{t^2(1-t^2)},\end{aligned}$$

(3.10)

$$S_{B_6}^0 : g^0(t,s) = s^2 + t^2 + 3 = 0.$$

It is noticeable that the equation $g^0(t,s) = 0$ of the base space $S_{B_6}^0$ coincides with the defining equation of the canonical model of the Shimura curve for discriminant 6 described in A. Kurihara[K]. Our computation for this family suggests that the field of definition of all endomorphisms of Jac$C(t,s)$ is not $\boldsymbol{Q}(t,s)$ but $\boldsymbol{Q}(t,s,\sqrt{R})$. Since this makes it impossible to determine the congruence ζ-function of $C(t,s)$ mod $\mathfrak{p}$ only from the number of $\boldsymbol{F}_q$-rational points ($q = N\mathfrak{p}$), $\mathcal{S}_6^0(t,s)$ is not suitable for our computation. For this reason we did not choose $\mathcal{S}_6^0(t,s)$ but $\mathcal{S}_6(t,s)$ for our computation.

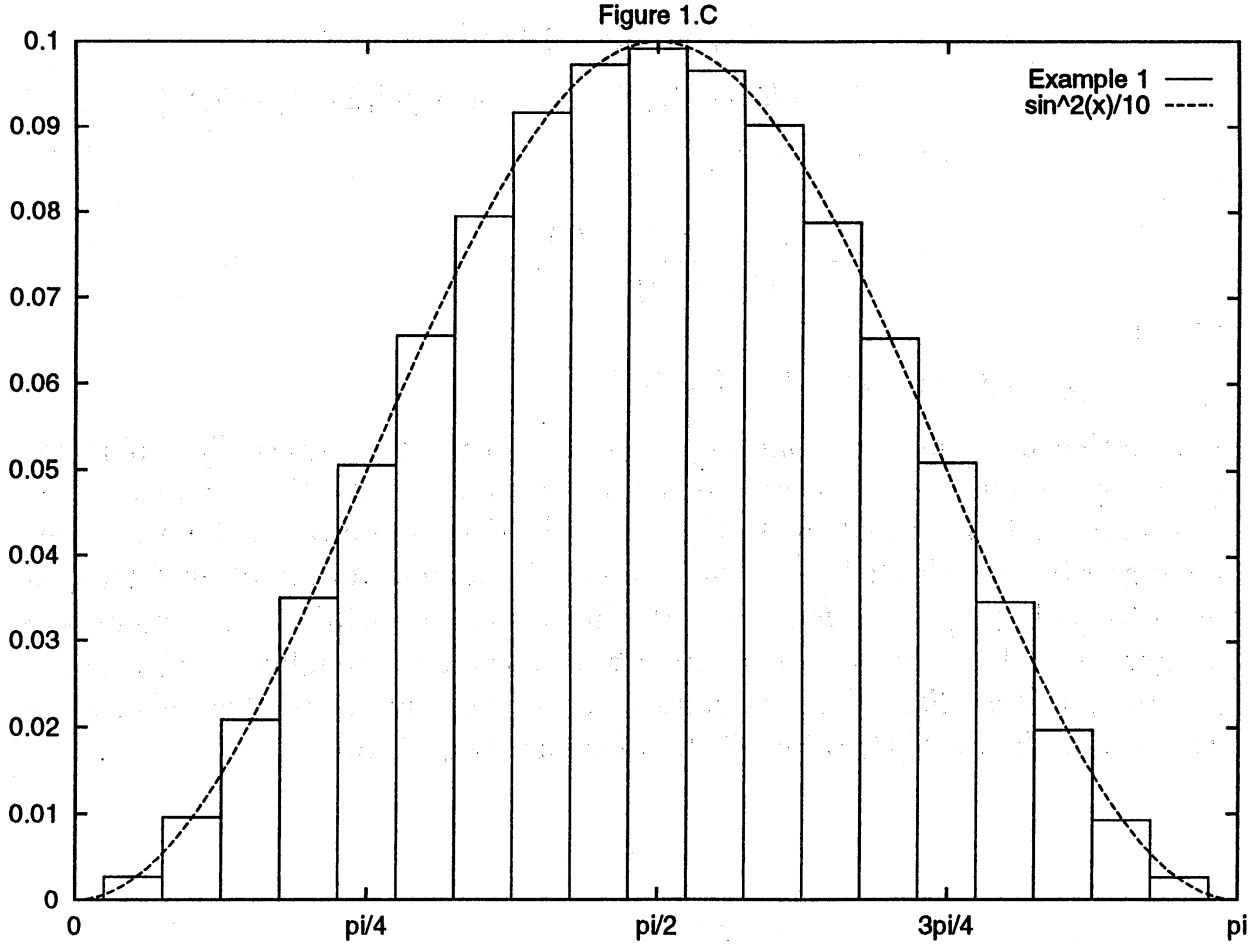
k	c_k
0	0.500000
1	0.002503
2	−0.500186
3	−0.002054
4	−0.002779
5	0.001513
6	0.000647
7	−0.002529
8	0.000754
9	−0.000483
10	0.002203
11	0.000223
12	−0.000862
13	0.000373
14	−0.001862
15	0.000216
16	−0.002844
17	−0.000214
18	0.006595
19	−0.003201
20	−0.002521

Table 1.A

i	range of θ	rel. frequency	$\frac{1}{10}\sin^2(\frac{i}{20}\pi)$
0	$0 < \theta < 0.025\pi$	0.000073	0.000000
1	$0.025\pi < \theta < 0.075\pi$	0.002682	0.002447
2	$0.075\pi < \theta < 0.125\pi$	0.009615	0.009549
3	$0.125\pi < \theta < 0.175\pi$	0.020858	0.020611
4	$0.175\pi < \theta < 0.225\pi$	0.034980	0.034549
5	$0.225\pi < \theta < 0.275\pi$	0.050584	0.050000
6	$0.275\pi < \theta < 0.325\pi$	0.065564	0.065451
7	$0.325\pi < \theta < 0.375\pi$	0.079453	0.079389
8	$0.375\pi < \theta < 0.425\pi$	0.091652	0.090451
9	$0.425\pi < \theta < 0.475\pi$	0.097286	0.097553
10	$0.475\pi < \theta < 0.525\pi$	0.099135	0.100000
11	$0.525\pi < \theta < 0.575\pi$	0.096575	0.097553
12	$0.575\pi < \theta < 0.625\pi$	0.090207	0.090451
13	$0.625\pi < \theta < 0.675\pi$	0.078742	0.079389
14	$0.675\pi < \theta < 0.725\pi$	0.065294	0.065451
15	$0.725\pi < \theta < 0.775\pi$	0.050927	0.050000
16	$0.775\pi < \theta < 0.825\pi$	0.034662	0.034549
17	$0.825\pi < \theta < 0.875\pi$	0.019781	0.020611
18	$0.875\pi < \theta < 0.925\pi$	0.009272	0.009549
19	$0.925\pi < \theta < 0.975\pi$	0.002633	0.002447
20	$0.975\pi < \theta < \pi$	0.000024	0.000000

Table 1.B

Figure 1.C



k	c_k
0	0.500000
1	−0.000028
2	−0.503450
3	0.000690
4	−0.000847
5	0.001115
6	0.007005
7	0.000266
8	−0.002776
9	−0.008435
10	−0.003711
11	0.007499
12	0.002184
13	0.000879
14	0.001389
15	−0.002216
16	0.001583
17	0.000991
18	−0.001262
19	0.000046
20	0.002469

Table 2.A

i	range of θ	rel. frequency	$\frac{1}{10}\sin^2(\frac{i}{20}\pi)$
0	$0 < \theta < 0.025\pi$	0.000098	0.000000
1	$0.025\pi < \theta < 0.075\pi$	0.002269	0.002447
2	$0.075\pi < \theta < 0.125\pi$	0.009648	0.009549
3	$0.125\pi < \theta < 0.175\pi$	0.020979	0.020611
4	$0.175\pi < \theta < 0.225\pi$	0.033127	0.034549
5	$0.225\pi < \theta < 0.275\pi$	0.048361	0.050000
6	$0.275\pi < \theta < 0.325\pi$	0.066656	0.065451
7	$0.325\pi < \theta < 0.375\pi$	0.082378	0.079389
8	$0.375\pi < \theta < 0.425\pi$	0.090477	0.090451
9	$0.425\pi < \theta < 0.475\pi$	0.094697	0.097553
10	$0.475\pi < \theta < 0.525\pi$	0.100576	0.100000
11	$0.525\pi < \theta < 0.575\pi$	0.098136	0.097553
12	$0.575\pi < \theta < 0.625\pi$	0.091062	0.090451
13	$0.625\pi < \theta < 0.675\pi$	0.078304	0.079389
14	$0.675\pi < \theta < 0.725\pi$	0.067266	0.065451
15	$0.725\pi < \theta < 0.775\pi$	0.050068	0.050000
16	$0.775\pi < \theta < 0.825\pi$	0.033981	0.034549
17	$0.825\pi < \theta < 0.875\pi$	0.020174	0.020611
18	$0.875\pi < \theta < 0.925\pi$	0.009379	0.009549
19	$0.925\pi < \theta < 0.975\pi$	0.002342	0.002447
20	$0.975\pi < \theta < \pi$	0.000024	0.000000

Table 2.B

k	c_k
0	0.500000
1	−0.000280
2	−0.501998
3	−0.000975
4	0.499924
5	−0.001571
6	−0.502599
7	−0.001873
8	0.499744
9	−0.002418
10	−0.501226
11	−0.001901
12	0.500802
13	−0.000221
14	−0.502897
15	−0.000873
16	0.500289
17	0.000625
18	−0.500966
19	−0.001550
20	0.497862

Table 3.A

i	range of θ	rel. frequency	$\frac{1}{10}\sin^2(\frac{i}{20}\pi)$
0	$0 < \theta < 0.025\pi$	0.011463	0.000000
1	$0.025\pi < \theta < 0.075\pi$	0.024742	0.002447
2	$0.075\pi < \theta < 0.125\pi$	0.025352	0.009549
3	$0.125\pi < \theta < 0.175\pi$	0.025010	0.020611
4	$0.175\pi < \theta < 0.225\pi$	0.025279	0.034549
5	$0.225\pi < \theta < 0.275\pi$	0.025047	0.050000
6	$0.275\pi < \theta < 0.325\pi$	0.024620	0.065451
7	$0.325\pi < \theta < 0.375\pi$	0.025364	0.079389
8	$0.375\pi < \theta < 0.425\pi$	0.024913	0.090451
9	$0.425\pi < \theta < 0.475\pi$	0.025145	0.097553
10	$0.475\pi < \theta < 0.525\pi$	0.526083	0.100000
11	$0.525\pi < \theta < 0.575\pi$	0.025023	0.097553
12	$0.575\pi < \theta < 0.625\pi$	0.024693	0.090451
13	$0.625\pi < \theta < 0.675\pi$	0.025340	0.079389
14	$0.675\pi < \theta < 0.725\pi$	0.024888	0.065451
15	$0.725\pi < \theta < 0.775\pi$	0.024779	0.050000
16	$0.775\pi < \theta < 0.825\pi$	0.025132	0.034549
17	$0.825\pi < \theta < 0.875\pi$	0.024986	0.020611
18	$0.875\pi < \theta < 0.925\pi$	0.024498	0.009549
19	$0.925\pi < \theta < 0.975\pi$	0.025108	0.002447
20	$0.975\pi < \theta < \pi$	0.012536	0.000000

Table 3.B

References

[F] Faltings,G., Endlichkeitssätze für abelsche Varietäten über Zahlkörpern, Invent. Math. 73 (1983), 349–366.

[K] Kurihara,A., On some examples of equations defining Shimura curves and the Mumford uniformization, F. Fac. Sci. Univ. Tokyo, 25 (1979), 277–301.

[HM] Hashimoto,K., Murabayashi,N., Shimura curves as intersection of Humbert surfaces and defining equations of QM-curves of genus two, Tohoku Math. J. (to appear).

[HT] Hashimoto,K.,Tsunogai,H., On the Sato-Tate Conjecture for QM-curves of genus two, in preparation.

[T] Tate, J., Algebraic Cycles and Poles of Zeta Functions, in "Arithmetical Algebraic Geometry", (F.G. Schilling, ed.), Harper and Row, New York, 1965.

[Ya] Yamamoto, Y., On Sato Conjecture for two-dimensional abelian varieties (in Japanese), Number Theory Symposium at Kinosaki (1979), 236–244.

[Yo1] Yoshida,H., Mumford-Tate groups and its application to abelian varieties (in Japanese), "Shimura varieties and algebraic geometry" Symposium at Kinosaki (1983), 106–131.

[Yo2] Yoshida,H., On an Analogue of the Sato Conjecture, Invent. Math. 19 (1973), 261–277.